
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

VOX MARKETING GROUP,

Plaintiff,

v.

PRODIGY PROMOS, *et al.*,

Defendants.

**MEMORANDUM DECISION
AND ORDER**

Case No. 2:18-cv-632

Howard C. Nielson, Jr.
United States District Judge

Plaintiff Vox Marketing Group sued Defendants Prodigy Promos, L.L.C., Henhouse Designworks, L.L.C, and individual Defendants Jason Marsh, John Priday, Tyler Fredrickson, Eric Oldson, Spencer Oldson, Michael Perley, Jeffrey Johns, and Brooke Johns. Vox asserts a federal claim under the Computer Fraud and Abuse Act (the “CFAA”) and various state-law claims against Prodigy and the other Defendants. Prodigy also asserts various state-law claims, including several counterclaims against Vox and some of its officers and employees as well as a claim against Alex Wolfe, a Vox employee.

Defendants move for summary judgment on Vox’s claims. And Vox (along with its officers and employees) moves for summary judgment on all of Prodigy’s claims. The court denies Defendants’ motion for summary judgment on Vox’s federal claim and declines to exercise supplemental jurisdiction over the state-law claims asserted in this case—including Vox’s other claims and all of Prodigy’s claims.

I.

Prodigy Promos, L.L.C., and Vox Marketing Group are both promotional and marketing companies. *See* Dkt. No. 208-1, Exhibit 1 ¶¶ 2–3. They are direct competitors. *See id.* ¶ 3; Dkt. No. 2-4 ¶ 19.

Vox uses a website, voxmarketingtools.com, to generate different types of documents that it uses in its relationships with its customers. *See* Dkt. No. 2-4 ¶ 75. These include

OrderPrint pages and PrintDelivery pages. OrderPrint pages are proposals (which include proposed pricing) that Vox provides its customers. *See id.* ¶¶ 76–77. PrintDelivery pages are packing lists that Vox provides with products that it ships to its customers. *See* Dkt. No. 208-1, Exhibit 1 ¶ 6; Dkt. No. 208-1, Exhibit 8 ¶ 13.

Vox intended for the documents generated by voxmarketingtools.com to be password protected. And individuals who type the address for the website’s homepage into an internet browser do encounter a login portal that requires a username and password to gain access to the website. *See* Dkt. No. 241 at 35; Dkt. No. 252 at 5, 11; and Dkt. No. 241-1 at 33, 107, and 152. In addition, this website was originally coded to require that individuals who type in URLs for specific documents generated by the website enter their username and password to gain access to the documents unless they are already validly logged into voxmarketingtools.com. At some point this feature became disabled, however, and individuals who typed in the URLs for specific OrderPrint and PrintDelivery documents could gain access to those documents without first entering a username and password. *See* Dkt. No. 2-4 ¶¶ 79–81.

In the summer of 2015, Prodigy obtained an OrderPrint page, presentations, and other documents that Vox had prepared for SolarCity, one of Vox’s customers. *See* Dkt. No. 208-1, Exhibit 1 ¶¶ 4–5. The parties dispute how Prodigy obtained these documents. Vox argues that Prodigy obtained them illegally through a kickback scheme with one of SolarCity’s employees. *See* Dkt. No. 2-4 ¶¶ 50-63. Defendants argue that SolarCity provided the documents to them to see whether Prodigy could offer competitive pricing. *See* Dkt. No. 208-1, Exhibit 1 ¶ 4. The URL for the OrderPrint document was printed at the top of the document. *Id.* ¶ 5.

This URL appears to have focused Defendants’ attention on the voxmarketingtools.com website. *See, e.g.,* Dkt. No. 196-1 at 32 48:15–49:4. Defendants proceeded to experiment with this website. They discovered that when they went to the website’s homepage, they would encounter a login portal that required a username and password. *See* Dkt. No. 241 at 35; Dkt. No. 252 at 5, 11; Dkt. No. 241-1 at 33, 107, 152. They also discovered that they could view the webpage showing the OrderPrint proposal they had obtained from SolarCity without first

entering a username and password by directly entering the URL for this specific document. *See* Dkt. No. 208-1, Exhibit 3 ¶¶ 12–13; Dkt. No. 196-1, Exhibit C at 100:8–101:15; Exhibit D at 49:5–12. With further experimentation, Defendants learned that by altering the numbers at the end of the URL they could also obtain access to different OrderPrint and PrintDelivery documents without entering a username or password. *See* Dkt. No. 208-1, Exhibit 8 ¶ 13; Exhibit 3 ¶11. And as they continued to experiment, Defendants gained sufficient insight into how the voxmarketingtools.com URLs were assigned to be able to locate OrderPrint and PrintDelivery documents based on when they were generated. *See id.* Exhibit 3 ¶11; Exhibit 8 ¶14.

Because Vox was a direct competitor, its pricing proposals were extremely valuable to Prodigy. Indeed, Prodigy’s employees described their ability to access OrderPrint and PrintDelivery pages as “freaking sneaky” and the “holy grail of spy tricks.” Dkt. No. 239-1, Exhibit 34 at 82. And Prodigy’s employees used this “holy grail” extensively, viewing various OrderPrint and PrintDelivery pages over twenty thousand times. *See* Dkt. No. 208-1, Exhibit 11 at 242.

Vox discovered these intrusions when it was told by a customer that, shortly after receiving a proposal from Vox, the customer received an unsolicited proposal from Prodigy offering to sell the exact same items for a lower price. *See* Dkt. No. 196-2, Exhibit L at 55:13–57:22. Vox then searched its server records and discovered that computers using IP addresses traceable to Prodigy had obtained access to Vox’s OrderPrint and PrintDelivery webpages. *See* Dkt. No. 196-1, Exhibit K at 78:5–15. Vox obtained a court order authorizing the sheriff to enter Prodigy’s premises, identify all electronic storage media, take temporary possession of those media, and deliver them to Decipher Forensics, LLC. *See* Dkt. No. 196-2, Exhibits Q, S, T.

Vox then brought this suit, asserting that Defendants’ manipulation of the website URLs in order to gain access to Vox’s OrderPrint and PrintDelivery webpages violated the CFAA and that its use of the materials it obtained in this manner to compete against Vox violated the Utah Uniform Trade Secrets Act and constituted tortious interference with economic relations. Vox also alleges that Prodigy’s manipulation of the URLs to obtain access to Vox’s webpages, as

well as the alleged kickback scheme through which Prodigy allegedly obtained the URL for the SolarCity OrderPrint page in the first place, violated the Utah Pattern of Unlawful Activity Act. Prodigy, in turn, asserts that the seizure of its devices and their delivery to a third-party company constituted trespass to chattels, and that Vox's application to the court for authorization to proceed in this manner constituted abuse of process. Prodigy also asserts a claim for defamation based on statements allegedly made to customer representatives by a Vox employee that Prodigy had hacked into or otherwise gained unauthorized access to Vox's system.¹ Finally, Prodigy asserts a claim for breach of contract against Alex Wolfe, a Vox employee, who it alleges solicited Prodigy customers for Vox after Prodigy terminated his employment.

II.

Under Federal Rule of Civil Procedure 56(a), "[t]he court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Material facts are those which "might affect the outcome of the suit under the governing law." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). A "dispute about a material fact is 'genuine' if the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Id.* (cleaned up). "Courts are required to view the facts and draw reasonable inferences in the light most favorable to the party opposing the summary judgment motion." *Scott v. Harris*, 550 U.S. 372, 378 (2007) (cleaned up).

III.

The court will begin by addressing Defendants' motion for summary judgment on Vox's CFAA claim. As noted, Vox contends that Defendants' manipulation of the website URLs in order to gain access to Vox's OrderPrint and PrintDelivery webpages violated this federal

¹ Prodigy also asserted claims for interference with economic relations and negligence based on Vox's response to Prodigy's access to the voxmarketingtools.com website, but it has not opposed Vox's motion for summary judgment on either of these claims.

statute. For the reasons that follow, the court denies Defendants’ motion for summary judgment on this claim.

A.

The CFAA imposes criminal penalties on anyone who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.” 18 U.S.C. § 1030(a)(2). A “protected computer” is defined broadly to include any computer “which is used in or affecting interstate or foreign commerce or communication.” *Id.* § 1030(e)(2)(B).

The CFAA also creates a private right of action for “[a]ny person who suffers damage or loss by reason of a violation of this section.” *Id.* § 1030(g). The CFAA provides specific definitions for “damages” and “loss.” “[T]he term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information.” *Id.* § 1030(e)(8). And “the term ‘loss’ means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” *Id.* § 1030(e)(11).

The CFAA further restricts the class of individuals who may bring a civil claim. As relevant here, Vox may bring suit only if it suffered a “loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value.” *Id.* § 1030(c)(4)(A)(i)(I); *see also id.* § 1030(g).

B.

Defendants argue that because they were not required to enter passwords to obtain access to the OrderPrint and PrintDelivery webpages, they did not “access a computer without authorization.” Defendants also contend that Vox did not suffer a loss—as defined by the CFAA—of at least \$5000 within a one-year period. The court concludes that genuine disputes of material fact preclude summary judgment for Defendants on either ground.

1.

Defendants maintain that anyone who makes a computer, website, or webpage accessible through the internet necessarily authorizes access to it by any member of the public unless it is protected by a password portal. It follows, Defendants seem to argue, that one may only obtain access to a computer “without authorization” in violation of the CFAA by hacking a password. The court readily agrees that general public access is at least presumptively authorized to computers, websites, or webpages that are accessible through the internet without a password. But the court is not persuaded that this presumption is irrebuttable or that there is a *per se* rule that one can never obtain access to a computer “without authorization” except by hacking a password.

To be sure, in *Van Buren v. United States*, the Supreme Court endorsed a “gates-up-or-down” inquiry to determine whether an individual’s access to a computer was “without authorization” under the CFAA, explaining that “one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.” 141 S. Ct. 1648, 1658–59 (2021). But the court expressly declined to decide whether “this inquiry turns only on technological (or ‘code-based’) limitations on access, or instead also looks to limits contained in contracts or policies.” *Id.* at 1659 n.8.²

Password protection, of course, is one example of a “technological (or ‘code-based’) limitatio[n] on access.” *Cf. id.* n.9 (describing password “authentication” as “a ‘specific type of authorization’”). And there can be no doubt that when a computer, website, or webpage is password protected, one who obtains access to information by hacking the password obtains access “without authorization.” It does not follow, however, that hacking a password is the *only* way that one can obtain access “without authorization.” As explained, this proposition is not

² The Court did reject the proposition that an individual who is authorized to access information for certain purposes “exceeds authorized access” when he violates contractual terms barring the use of information for other purposes. But, as noted, the Court explicitly left open the possibility that an individual could obtain access to information without authorization by violating contractual provisions barring any access at all to that information.

supported by *Van Buren*. And the court does not understand any of the cases cited by the parties—or any other cases that it has found—to support this categorical proposition.

None of the cases cited by Defendants address factual circumstances comparable to those presented here. For example, Defendants cite *Healthcare Advocates, Inc. v. Harding, et al.*, 497 F. Supp. 2d 627 (E.D. Pa. 2007), in support of their claim that “[a]ccess is inherently authorized on an open webpage.” Dkt. No. 208 at 26. In *Healthcare Advocates*, the defendant law firm was able to obtain access to some of the plaintiff’s archived webpages through a webpage archiving service known as the Wayback Machine. Even though the plaintiff, and the Wayback Machine service itself, had intended for access to these webpages to be blocked through an opt-out function, that function sometimes malfunctioned. To be sure, the court in that case did find that the defendant’s access to these pages was authorized. The court emphasized, however, that the defendant did nothing wrongful, and indeed did nothing at all other than use the Wayback Machine in the usual manner. 497 F. Supp. 2d at 648–49. As the court explained, the defendant “accessed the Internet Archive’s website with only an ordinary web browser,” “they did not employ any special tools,” and on those occasions that the opt-out function blocked their access to some of the plaintiff’s webpages, they made no attempt “to get past the blocking mechanism.” *Id.* at 648. The court likewise emphasized that the defendants were unaware that the Wayback Machine had malfunctioned or that the plaintiff intended to block public access to the webpages they viewed. *Id.* at 648–49. Finally, the court made clear its view that “[c]ircumventing an electronic protective measure violates federal law.” *Id.* at 633. For all of these reasons, *Healthcare Advocates* does not support the categorical proposition urged by Defendants.

Nor is the court convinced that this categorical proposition is sound. While it certainly may be true in most cases that general public access to computers connected to the internet is authorized when the computer is not password protected, it is easy enough to imagine circumstances in which this general rule seems not to hold true. For example, if an employee at an office left her computer open while stepping out for a few minutes, it would certainly seem that access to that computer and its files by another individual while the employee was gone

would be “without authorization”—even if the computer and the files were not password protected.

In this case, it is undisputed that someone seeking access to an OrderPrint proposal or PrintDelivery document through the voxmarketingtools.com homepage would be required to enter a username and password. And it is undisputed that at least some of Vox’s employees visited the homepage and saw the password portal. It is also undisputed that at the relevant time someone entering the URL for a specific OrderPrint or PrintDelivery document could obtain access to that document without providing a username and password. But while it is disputed how Prodigy obtained the OrderPrint proposal for SolarCity—which included the URL for that specific document—it is undisputed that Vox did not provide Defendants the URLs for the thousands of other OrderPrint proposals and PrintDelivery documents viewed by Defendants. The record also strongly supports an inference that Defendants knew these documents contained sensitive information that Vox did not intend to make generally available to the public. Under these circumstances, the court believes that unless there is a *per se* rule that one can never violate the CFAA by obtaining access to a protected computer “without authorization” except by hacking a password—a proposition the court has already rejected—genuine disputes of material fact preclude summary judgment for Defendants.

First, there is a factual dispute regarding whether Defendants employed unlawful means to obtain the OrderPrint proposal that focused their attention on the voxmarketingtools.com website and provided them the specific URL that launched their experimentation. If Defendants’ access to the proposal and the URL was itself unlawful, the court believes that a reasonable jury could find on that ground alone that their manipulation of the unlawfully obtained URL to obtain access to other OrderPrint proposals was “without authorization.” On the other hand, if Defendants obtained the OrderPrint proposal in a lawful manner, simply typing the URL printed on the proposal into a web browser and viewing the associated webpage probably would not, without more, violate the CFAA. After all, it seems reasonable to assume that by printing the URL on the proposal, Vox authorized access to the associated website by the lawful recipient of

the proposal. But it does not follow that by printing a single URL on this proposal Vox authorized a lawful recipient of the proposal to obtain access to *different* documents by manipulating the URL.

In addition, the court concludes that a reasonable jury could find that Defendants knew that Vox intended the OrderPrint proposals and PrintDelivery documents to be password protected based on the obviously sensitive nature of the information they contained as well as the undisputed fact that at least some of Defendants' employees knew that the homepage of the voxmarketingtools.com website contained an active password portal and that it was thus impossible to obtain access to the OrderPrint proposals and Print Delivery documents through the homepage of the website except by entering a username and password. Under these circumstances, the court is not convinced that obtaining access to the OrderPrint proposals and PrintDelivery documents by guessing their likely URLs based on one example is materially different from obtaining access to a password-protected computer or webpage by guessing a password, perhaps based on a clue inadvertently disclosed by the authorized user. Nor is the court convinced that obtaining access by manipulating the URLs under these circumstances is materially different from obtaining access to a password-protected website or webpage by means of a computer that an authorized user has inadvertently failed to log out. In any of these circumstances, the court believes that a reasonable jury could find intentional circumvention of password protection and access without authorization.

In short, viewing the facts in the light most favorable to Vox and drawing all reasonable inference in its favor, the court concludes that a reasonable jury could find that Defendants knew that Vox intended the OrderPrint and PrintDelivery pages to be password protected but that the password protection was not completely effective, and that Defendants nevertheless knowingly exploited the defect in the password protection to obtain access to the OrderPrint and PrintDelivery pages. Viewed in this manner, Defendants' knowledge seems comparable to that of someone who learns that the locking mechanism of a physical door does not securely engage when the door is locked and shut, and that the door can thus be opened by rattling the handle or

the door itself until the lock disengages. And just as one who knowingly goes through a locked door in such a manner is no more authorized to enter than someone who picks the lock, the court believes that a reasonable jury could find that Defendant was no more authorized to obtain access to the OrderPrint proposals and PrintDelivery documents by knowingly exploiting a defect in Vox's password protection than it would have been to obtain access to these proposals by hacking a password.

For all of these reasons, the court concludes that genuine disputes of material fact preclude summary judgment for Defendants on the CFAA claim on the ground that their access to the OrderPrint and PrintDelivery pages was authorized.

2.

Defendants also argue that Vox "has not suffered an actionable 'damage' or 'loss' for purposes of the CFAA." Dkt. No. 208 at 30. As noted, Plaintiff must have incurred a "loss" within a one-year period "aggregating at least \$5,000 in value" to bring a claim under the CFAA. 18 U.S.C. § 1030(c)(4)(A)(i)(I). And as also noted, the CFAA defines the term "loss" to mean "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11); *see also id.* § 1030(e)(8) (defining "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information"). Defendants argue that Plaintiff has failed to present evidence that it incurred costs of at least \$5000 as defined by the statute.

Defendants rely on the deposition testimony of Vox's COO, Aaron Scott, who discussed costs that Vox incurred "analyzing what information Defendants obtained and how they might have used it." Dkt. No. 252 at 17. Mr. Scott testified that this included

a lot of analyzing of the server logs, trying to find their patterns, how Jason passed the information to—and why the particular interest, studying patterns, doing things like that. Running queries to look at all the hits for a particular customer to try to understand their interest or what they were looking at what they were doing. Things like that.

Dkt. No. 208-1, Exhibit 4 at 224:21-24. Defendants argue that costs that Vox incurred in conducting such an analysis do not fall within the statutory definition of “loss.”

The court need not decide whether Defendants correctly interpret the statutory definition, however. Mr. Scott stated in his declaration that Vox also incurred \$6,000-\$7,000 in costs consisting

primarily of the time of Vox employees . . . we investigated the nature of the attack . . . we took all of the machines on our network out of service, one-by-one, and reviewed and tested them to determine if they had been compromised by defendants . . . we basically de-commissioned and re-commissioned every machine in the network . . . we shifted the numerical range of our live orderprint pages to prevent further access by the defendants.

Dkt. No. 239-1, Exhibit 28 ¶ 32. This declaration is consistent with his deposition testimony:

Q: Okay. And then tell me about the audit performed after Vox learned that Prodigy was viewing proposals and delivery receipts.

A: So we took each computer out of the configuration one at a time and ran tests on it, antivirus, malware, spyware. We checked everything. In some cases, we reloaded the software and we just went through the whole configuration one by one.

. . .

Q: And how is it that Vox calculates the damage done to Vox’s computers to be in excess of \$5,000?

A: Based on the time and resources it took to go through everything, and you, know, audit—the audit we have spoken about.

Dkt. No. 208-1, Exhibit 4 at 181:1–9, 221:2–8; *see also id.* at 221:20 (estimating that Vox spent “between 6- and \$7,000” on the audit).

Significantly, when discussing the costs that Vox incurred analyzing what information Defendants obtained and how they might have used it, Mr. Scott testified at his deposition that these costs “would be much higher” than the \$6,000–\$7,000 in costs Vox incurred auditing its computers to determine how Defendants obtained access to them and whether they were compromised in anyway. *Id.* at 224:3–5.

Although Mr. Scott’s deposition testimony is not a model of clarity, viewing the testimony as a whole and in the light most favorable to Vox, and drawing all reasonable inferences in Vox’s favor—as the court is required to do when determining whether Defendants

are entitled to summary judgment—the court concludes that Mr. Scott testified that Vox incurred two types of costs: (1) more than \$5000 in auditing its computers to determine how Defendants obtained access to them and whether they were compromised in anyway by Defendants, and (2) additional, and “much higher” costs analyzing why Defendants were interested in particular documents. Because there is no dispute that the first category of costs falls within the statutory definition of “loss,” the court concludes that Defendants are not entitled to summary judgment on the ground that Vox failed to present evidence that it incurred a “loss” within a one-year period “aggregating at least \$5,000 in value.”

IV.

The court next considers the various state law claims asserted by the parties in this case. The parties have not alleged that the court has diversity jurisdiction over these claims. *See, e.g.*, Dkt. No. 2 at 3–4 (notice of removal). Federal jurisdiction over these claims thus must be based on 28 U.S.C. § 1367.

As relevant here, this statute provides that
in any civil action of which the district courts have original jurisdiction, the district courts shall have supplemental jurisdiction over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

28 U.S.C. § 1367(a). As the Supreme Court has explained, this statute codifies

principles of pendent and ancillary jurisdiction by which the federal courts’ original jurisdiction over federal questions carries with it jurisdiction over state law claims that derive from a common nucleus of operative fact, such that the relationship between the federal claim and the state claim permits the conclusion that the entire action before the court comprises but one constitutional case.

City of Chicago v. International College of Surgeons, 522 U.S. 156, 164–65 (1997) (quoting *United Mine Workers v. Gibbs*, 383 US 715, 725 (1966)) (cleaned up).

Section 1367 also provides, however, that

district courts may decline to exercise supplemental jurisdiction over a claim under subsection (a) if—

- (1) the claim raises a novel or complex issue of State law,
- (2) the claim substantially predominates over the claim or claims over which the district court has original jurisdiction,

(3) the district court has dismissed all claims over which it has original jurisdiction, or

(4) in exceptional circumstances, there are other compelling reasons for declining jurisdiction.

28 U.S.C. § 1367(c). Thus, “[e]ven where a ‘common nucleus of operative fact’ exists, federal jurisdiction is not mandatory over pendent claims or parties.” *Estate of Harshman v. Jackson Hole Mountain Resort Corp.*, 379 F.3d 1161, 1165 (10th Cir. 2004). Rather, “supplemental jurisdiction is not a matter of the litigants’ right, but of judicial discretion.” *Id.*

In this case, the court has little difficulty concluding that Prodigy’s claim against Mr. Wolfe for breach of contract does not arise from the same “common nucleus of operative fact” as Vox’s CFAA claim. Indeed, the claim does not appear to have any relationship to Prodigy’s access to the OrderPrint and PrintDelivery documents. Rather, this claim is based on allegations that Mr. Wolfe, a Vox employee who had previously worked for Prodigy and signed Confidentiality and Non-Circumvention agreements, “materially breached the Agreements by, among other things, soliciting Prodigy customers, using and disclosing Prodigy’s confidential information, and assisting Vox in using Prodigy’s confidential information.” Dkt. No. 2-7 ¶ 33. The court thus lacks supplemental jurisdiction over this claim.

Although it is a much closer question, the court also has at least some doubt regarding supplemental jurisdiction over Prodigy’s remaining claims. To be sure, these claims may have some loose connection with the CFAA claim, but they arise out of the actions Vox took *after* it discovered Prodigy’s access to the OrderPrint and PrintDelivery documents rather than the access itself.

The court need not decide this issue, however. For even if the court has supplemental jurisdiction over these counterclaims, it declines to exercise supplemental jurisdiction over any of the state-law claims asserted by the parties.

As noted, the court may decline to exercise supplemental jurisdiction if “the claim raises a novel or complex issue of State law.” 28 U.S.C. § 1367(c)(1). And several of the state law claims asserted in this case do raise such issues.

It is unclear, for example, whether Utah even recognizes the tort of trespass to chattels, let alone what the elements of this tort might be under Utah law. *See* Dkt. No. 196 at 30. In addition, Plaintiff’s claim under the Utah Pattern of Unlawful Activity Act presents a difficult and unanswered question about what constitutes a “substantial period of time” for purposes of the Act. *See* Dkt. No. 241 at 55–56. And whether the documents to which Prodigy obtained access constitute “trade secrets” for purposes of Vox’s claim under Utah’s Uniform Trade Secrets Act presents a “complex issue of State law.” *See id.* at 38–44.

The court may also decline to exercise supplemental jurisdiction over a state law claim if “the claim substantially predominates over the claim or claims over which the district court has original jurisdiction.” 28 U.S.C. § 1367(c)(2). The court concludes that this is the case for all of the state law claims asserted here.

The CFAA claim here presents the discrete legal issue of whether Prodigy’s access to Vox’s webpages was “without authorization.” And if Vox prevails on this claim, its “damages” appear limited to compensation for “impairment to the integrity or availability of data, a program, a system, or information,” 18 U.S.C. § 1030(e)(8); *see also id.* § 1030(g), and, presumably, reasonable costs that it incurred “responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service,” *id.* § 1030(e)(11). As discussed, the evidence in this case suggests that Vox may well be limited to recovering \$6000–\$7000 if it prevails on this claim.

Although some of the issues raised by the state-law claims may overlap with the issue raised by the CFAA claim, all of the state-law claims raise other, more numerous issues, including such significant issues as whether the information Prodigy obtained included trade secrets, how Prodigy used this information, whether Prodigy’s use of this information resulted in Vox losing customers to Prodigy, whether Prodigy and the other Defendants engaged in a pattern of unlawful conduct, and whether Vox’s response to Prodigy’s actions was reasonable and

lawful. In addition, the parties seek hundreds of thousands of dollars in damages for these state-law claims.

Whether viewed legally in terms of the number and complexity of the specific issues raised or practically in terms of real-world stakes, there can thus be no doubt that each of the state-law claims “substantially predominates over” the single and discrete federal claim “over which the district court has original jurisdiction.” Exercising federal jurisdiction over the high-economic-stake, complex, and predominantly state-law disputes among the parties to this action based solely on a discrete CFAA claim likely worth only several thousand dollars would permit a small, federal-law tail to wag an enormous, state-law dog. That is not how our dual system of state and federal courts should work.

The court thus declines to exercise supplemental jurisdiction over the state-law claims at issue in this case. No later than September 3, 2021, the parties may submit briefing addressing (1) whether the court should dismiss these claims without prejudice or should instead remand them to the state court from which this action was removed, and (2) if remand is appropriate, whether the court may remand these claims now or must instead wait until it has resolved the CFAA claim. *See Carnegie-Mellon University v. Cohill*, 484 U.S. 343, 351 (1988).

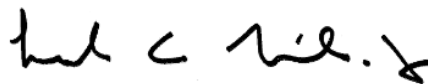
* * *

For the foregoing reasons, Defendants’ motion for summary judgment on Vox’s CFAA claim is **DENIED**. The court declines to exercise supplemental jurisdiction over the parties’ state-law claims.

IT IS SO ORDERED.

DATED this 20th day of August, 2021.

BY THE COURT:



Howard C. Nielson, Jr.
United States District Judge